The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2/8/2011

SUBJECT:
Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (MS11-007)

OVERVIEW:

A vulnerability has been discovered in the Microsoft Windows OpenType Compact Font Format driver that could allow for remote code execution. OpenType Fonts are fonts that get embedded in documents such as Microsoft Word, Power Point, or Web pages. These vulnerabilities can be exploited if a user visits a specially crafted webpage or opens a specially crafted file, including e-mail attachments.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Microsoft Windows OpenType Compact Font Format (CFF) driver. The vulnerability is caused due to the Windows OpenType Compact Font Format (CFF) driver not properly validating the parameter values of specially crafted OpenType fonts.

On Windows Vista, Windows Server 2008, and Windows 7, an attacker could leverage this issue by persuading a user to visit a specially crafted web site with an embedded, specially crafted OpenType font. In an email based attack scenario, the user would have to open a specially crafted OpenType font as an email attachment. On Windows XP and Windows Server 2003, an attacker would first need to login to the affected system. Once logged in, they would then need to run a specially crafted application to exploit this vulnerability.

It should be noted that, by default, Internet Explorer is not affected by this vulnerability. However, other third-party web browsers that natively render OpenType fonts are vulnerable.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patches provided by Microsoft immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS11-007.mspx

Security Focus:
http://www.securityfocus.com/bid/46106

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0033